REMARKS

With this amendment the independent claim 1 and dependent claim 6 have been amended, claims 9-13 have been cancelled and claims 14-19 have been added. Of the added claims 15-19 are method claims. Independent claims 1, 14 and 15 are pending. Applicants and their attorney thank Examiners Au and Zimmerman for the interview of January 10, 2008. Applicants will understand if the method claims are subjected to a restriction requirement. Claims 1, 14 and 15 presented herein are similar to the draft claim 14 discussed at the interview and noted on the interview summary. Indeed amended claim 1 is believed to be identical to the draft claim 14 discussed at the interview.

The Rejection – NON FINAL.

The last rejection was solely an obviousness rejection.

The Examiner asserts claims 1, 2, 5, 7-11 and 13 are obvious in view of Hasu (6,041,410), Flick (6,140,939 and Waraksa (5,412,379).

The rejection of dependent claim 3 added Nicholls (for the teaching of an electroluminescent fingerprint sensor).

The rejection of dependent claim 4 added Toyoda (for the teaching of charged coupled devices or CCDs).

The rejection of claim 6 added Fitzgibbon (5,751,224 for the teaching of a wall controller).

The Problem.

In the past, wireless security systems were vulnerable to code grabbers which would read and store codes from a transmitter being used to gain access to a secured area. Because of that problem, rolling code which changes the access code with each use of that code to gain access to a secured area has been used to defeat code grabbing. Transmitters using rolling code, however, can be lost or stolen. This also compromises security. Transmitters or security systems which relied solely on biometric data, such as finger prints, were thought nearly invulnerable. See Declaration of Fitzgibbon attached. That was not true as will be explained in more detail below. The claims herein describe a barrier

operator system and method which address and solves this security problem.

The Interview

Applicants' attorney indicated that historically, as noted above, the art viewed security based on finger print data (as well as other certain types of biometric data) as nearly invulnerable. See Declaration of Fitzgibbon. Hey, unless you cut off a finger, the bad guy does not get in. But that is not true and the art did not recognize this. Code grabbers can get wireless signals representative of finger prints just like any other non-rolling code door opener.

Second wireless transmitters for barrier operators can be lost or stolen. Security arising from transmitters permanently installed in automobile visors etc. present a particular security problem if the automobile is broken into. Applicants' barrier operator system solves these problems.

The art discussed at the interview included Hsu, Flick and Waraksa. Applicants' attorney also mentioned Scott which was not applied by the Examiners. The patent claim primarily discussed at the interview was a new claim. The elements of that new claim discussed at the interview now have been incorporated into claim 1. New claim 14 is very similar to claim 1 and generally has the elements of draft claim 14 discussed at the interview. The same is true of new independent method claim 15.

Finally, Examiner Zimmerman indicated an interest in having a declaration confirming the fact discussed at the interview that the general attitude of persons in the security art at the time this application was filed was that biometric data as a means for access to a secured area was about the best one could do in protecting the area from an unauthorized access by specific individuals.

The Claims Are Non-Obvious In View Of The Applied Art Hsu, Flick and Waraksa

None of the references alone or in combination teach or suggest a system that determines the acceptance of both a user fingerprint and a rolling code. Since elements of claim 1 are not taught or suggested by the prior art, it is believed that independent claims 1, 14 and 15 are allowable for this reason.

Hsu and Flick completely rely on the use of a signal representative of finger print data for entry

into a secured area. The prior art thought this form of entry was invulnerable. Waraksa has nothing to do with biometric data, but rather describes a portable beacon which transmits to a receiver/controller with RF signals.

None of these references address or solve a problem of when a bad guys cut off a finger electronically with a code grabber to obtain the code representative of finger print data. This compromises the security of the system. In this aspect, finger print access control is no better than any other non-rolling code barrier operator.

The system of the instant application recognizes the problem that if lost to a bad guy, the bad guy can use YOUR rolling code transmitter to get into the house or garage.

Hsu

Hsu only involves transmissions indicating valid fingerprints.

Examiner admits Hsu does not show a comparison of finger print at the operator. See page 3 of Office Action top. Hsu scans the finger print and compares: A person 12 has fingerprint scanned and compared to a reference print at fob 14. A confirming message is sent to door 12.

Hsu does not describe the use of codes except to say they are encrypted. Examiner Zimmerman suggested that this response address Hsu's use of public and private keys. That discussion starts at column 6, line 42 and continues to column 7, line 34. Hsu's discussion **does not suggest a combining and a separating a combined signal as claimed**. In the end there is one encrypted message which is decrypted which opens the door. There is no indication of combining codes, transmitting a combined code and then separating the combined code at the operator as claimed.

Finally Hsu does not ***suggest transmission of both rolling code and fingerprint data.***

Flick

Flick is only concerned with finger print identification and it is this fingerprint identification that provides the required security.

Flick scans the finger print and sends only that fingerprint data --a vehicle start controller 86

receives biometric sensor data from remote transmitter 50. There can be a comparison at the transmitter or operator, but so-what. ***There is NO teaching of transmitter 50 sending both a rolling code (which represents a particular transmitter) and finger print data.***

Flick does not suggest determining whether both fingerprint and rolling code are acceptable.

Flick does not suggest combining a code representative of the finger print with an access code and then splitting them.

Waraksa

Waraksa describes a passive keyless entry system. Transmitter 24 generates what the Examiner calls a rolling code, but this reference does not teach the use of both rolling code and fingerprint data or whether both are acceptable.

Waraksa does not teach combining a code representative of the finger print with an access code and then recognizing the access code and fingerprint code for access to a secure area. If the Examiner looks at column 8, lines 46 to 55 and column 10, lines 37 to 55, he will see that Waraksa describes a clock for which a clock code is generated and which changes. This is not a rolling code, but this is not terribly relevant because at the interview everyone acknowledged that rolling codes are known e.g. the Examiner could cite a Chamberlain patent such as 4,750,118 to Heitschel. The '118 patent has been cited to the Examiner in a very recent IDS which was filed with our last amendment.

But no one has suggested combining a fingerprint code with a changing access code and then recognizing the fingerprint code as something that needs to be identified at the operator.

The Examiner has stated that "Waraksa teaches a rolling code used to mix up the id or unlocking code of the portable device to prevent cloning and unauthorized access. Therefore, it would have been obvious... to have mixed a rolling code with the Hsu-Flick transmission since this would aid in preventing unauthorized access." That is not true, the art teaches it thought finger print data for security is invulnerable.

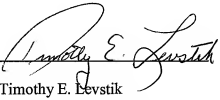
The prior art does not suggest combining a system that combines the use of signals

representative of finger print data to guard against the loss or theft of the transmitter and the use of rolling code to defeat code grabbers, as claimed.

The Commissioner is hereby authorized to charge any additional fees which may be required in this Application to Deposit Account No. 06-1135.

Respectfully requested,

FITCH, EVEN, TABIN & FLANNERY

By 

Timothy E. Levstik
Registration No.: 30,192

Date: February 28, 2008

Fitch, Even, Tabin & Flannery
120 South LaSalle Street
Suite 1600
Chicago, Illinois 60603-3406
Telephone: (312) 577-7000
Facsimile: (312) 577-7007